



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/004,301

11/02/2001

Bridget J. Frey

PLM007001

8153

30349

7590

08/08/2006

JACKSON & CO., LLP
6114 LA SALLE AVENUE
SUITE 507
OAKLAND, CA 94611-2802

EXAMINER

CERVETTI, DAVID GARCIA

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 08/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/004,301	Applicant(s) FREY ET AL.	
	Examiner David G. Cervetti	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 May 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5, 8-15, 17-21, 24-31, 33-37, 40-47 and 49-84 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5, 8-15, 17-21, 24-31, 33-37, 40-47 and 49-84 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 June 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Applicant's arguments filed May 19, 2006, have been fully considered but they are not persuasive.
2. Claims 1-5, 8-15, 17-21, 24-31, 33-37, 40-47, and 49-84 are pending and have been examined.
3. Claims 6-7, 16, 22-23, 32, 38-39, and 48 have been canceled.

Response to Amendment

4. Regarding Applicant's argument that Cohen does not disclose multiple SSO server, Examiner points Applicant's attention to column 9, lines 17-67, column 10, lines 20-45, where Cohen clearly teach multiple SSO servers and suggests a more distributed configuration for the system. Cohen clearly teaches signing on to multiple targets and domains. Furthermore, it is respectfully submitted that the number of single-sign-on servers used does not determine patentability. Adding more single-sign-on servers to Cohen does not patentably distinguish Cohen from the instant application.
5. Assuming *arguendo* Cohen does not expressly disclose that feature, Examiner respectfully submits that Cohen does not limit his invention to be **ONE AND ONLY ONE** single-sign-on server, but allows for a chaining of servers, since the targets on SSO server A are not limited to only resources other than SSO servers, therefore one such target resource could be another single-sign-on server. Cohen further discloses using the username, the password, and the domain for each target to sign on (column 12).
6. Assuming *arguendo* Cohen does not teach/disclose any of the claimed features, Examiner respectfully submits that using a temporarily assumed base, primitive single-

Art Unit: 2136

sign-on system of Cohen, it would have been obvious to someone of ordinary skill in the art to replace the authentication mechanism/scheme performed by Cohen with other schemes, based on the definition of a single-sign on system/mechanism, that is enabling users to authenticate once to gain access to network resources (multiple systems). How many layers of authentication – to provide more security (confidentiality, integrity, and availability) – are placed between the end user and the end resources is irrelevant, since the base system already provides the services.

Claim Objections

7. Claims 79-81 and 82-84 are objected to because of the following informalities: both recite the same limitations and are both dependent (directly or indirectly) of the same independent claim (claim 47). Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1, 8, 12, 15, 17, 24, 33, 40, 44, and 47 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 8, 12, 15, 17, 24, 33, 40, 44, and 47 recite the limitation "the server". There is insufficient antecedent basis for this limitation in the claims (there are an "enterprise server" and a plurality "resource server").

Claims 24 and 40 recite the limitation "the first SSO credential". There is insufficient antecedent basis for this limitation in the claims.

This may not be a complete list of insufficient antecedent issues in the claims.

10. Claim 24 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential elements, such omission amounting to a gap between the elements. See MPEP § 2172.01. The omitted elements are:

- means for receiving at the server a signal representing a first single-sign-on (SSO) credential generated by a first SSO provider based on the logon credential;
- means for sending from the server a signal representing the first SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the first SSO credential.

Claim Rejections - 35 USC § 101

11. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

12. Claims 24, 62-68 are rejected under 35 U.S.C. 101 because the disclosed invention is inoperative and therefore lacks utility. A first SSO credential was never generated, therefore the second SSO credential does not exist. Claims 62-68 are rejected based on their dependency from claim 24. For the purposes of this document Examiner has interpreted claim 24 to be the “apparatus” version of the “computer-implemented method” of claim 8 and of the “computer-readable media tangibly embodying a program” of claim 40.

Claim Rejections - 35 USC § 102

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

14. **Claims 1-5, 8-15, 17-21, 24-31, 33-37, 40-47, and 49-84 are rejected under 35 U.S.C. 102(e) as being anticipated by Ramamurthy et al. (US Patent 7,080,077, hereinafter Ramamurthy).**

Regarding claims 1, 17, and 33, Ramamurthy teaches

- storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol (column 7, column 8, lines 3-41);
- maintaining a map between one or more resource servers and a type of security credential required to access each resource server (column 8, lines 3-41);
- receiving at the enterprise server a signal representing a request from the remote user for a first of the secure resources, wherein the request includes a logon credential for the remote user (column 8, lines 3-41);

- determining, by referring to the map and without the intervention of the user, the type of security credential for the remote user that is required to access the first secure resource (column 8, lines 3-41); and
- sending from the server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security credentials for the user of the type required to access the first secure resource (column 8, lines 3-41);
- receiving at the server a signal representing a first single-sign-on (SSO) credential generated by a first SSO provider based on the logon credential (column 8, lines 3-41);
- sending from the server a signal representing the first SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the first SSO credential (column 8, lines 3-41); and
- sending from the server a signal representing the first SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes a second SSO credential corresponding to a second SSO provider having a trust relationship with the first SSO provider (column 34, lines 42-67, column 48, lines 38-67, column 49, lines 1-45).

Regarding claims 12 and 44, Ramamurthy teaches

- storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol (column 7, column 8, lines 3-41);
- maintaining a map between one or more resource servers and a type of security credential required to access each resource server (column 8, lines 3-41);
- receiving at the enterprise server a signal representing a request from the remote user for a first of the secure resources, wherein the request includes a Logon credential for the remote user (column 8, lines 3-41);
- determining, by referring to the map and without the intervention of the user, the type of security credential for the remote user that is required to access the first secure resource (column 8, lines 3-41);
- sending from the server a signal representing a second request to retrieve the first secure resource. the second request including a first of the security credentials for the user of the type required to access the first secure resource, wherein the receiving includes receiving at the server a signal representing a third request from the remote user for a second of the secure resources residing on the network (column 8, lines 3-41),

- determining, without the intervention of the user, the type of security credential for the remote user that is required to access the second secure resource (column 8, lines 3-41); and
- sending from the server a signal representing a fourth request for retrieving the second secure resource, the fourth request including a second of the security credentials for the user of the type required to access the second secure resource (column 8, lines 3-41); and
- wherein the signals representing the second and fourth requests are sent concurrently (column 8, lines 3-41, column 48, lines 38-67, column 49, lines 1-45).

Regarding claims 15 and 47, Ramamurthy teaches

- storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol (column 7, column 8, lines 3-41);
- maintaining a map between one or more resource servers and a type of security credential required to access each resource server (column 7, column 8, lines 3-41);
- receiving at the enterprise server a signal representing a request from the remote user for a first of the secure resources, wherein the request includes a logon credential for the remote user (column 7, column 8, lines 3-41);

- determining, by referring to the map and without the intervention of the user, the type of security credential for the remote user that is required to access the first secure resource (column 7, column 8, lines 3-41);
- sending from the server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security credentials for the user of the type required to access the first secure resource (column 7, column 8, lines 3-41),
- receiving at the server a signal representing the first security credential from the user before receiving the signal representing the first request (column 7, column 8, lines 3-41, column 48, lines 38-67, column 49, lines 1-45).

Regarding claims 8, 24, and 40, Ramamurthy teaches

- storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol (column 7, column 8, lines 3-41);
- maintaining a map between one or more resource servers and a type of security credential required to access each resource server (column 7, column 8, lines 3-41);
- receiving at the enterprise server a signal representing a request from the remote user for a first of the secure resources, wherein the request

- includes a logon credential for the remote user (column 7, column 8, lines 3-41);
- determining, by referring to the map and without the intervention of the user, the type of security credential for the remote user that is required to access the first secure resource (column 7, column 8, lines 3-41, column 48, lines 38-67, column 49, lines 1-45);
 - sending from the server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security credentials for the user of the type required to access the first secure resource (column 7, column 8, lines 3-41);
 - receiving at the server a signal representing a first single-sign-on (SSO) credential generated by a first SSO provider based on the logon credential (column 7, column 8, lines 3-41);
 - sending from the server a signal representing the first SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the first SSO credential (column 7, column 8, lines 3-41);
 - receiving at the server a signal representing a second SSO credential generated by a second SSO provider based on the first SSO credential (column 48, lines 38-67, column 49, lines 1-45); and
 - sending from the server a signal representing the second SSO credential to retrieve the first secure resource when the type of credential required

to access the first secure resource includes the second SSO credential
(column 48, lines 38-67, column 49, lines 1-45).

Regarding claims 2, 18, 34, 49, 69, Ramamurthy teaches

- authenticating the user before sending the signal representing the second request (column 7, column 8, lines 3-41).

Regarding claims 3, 19, 35, 50, 70, Ramamurthy teaches

- receiving at the server a signal representing a response to the second request; and
- sending from the server a signal representing a result to the remote user, the result based on the response to the second request (column 8, lines 42-67, column 9, lines 1-45).

Regarding claims 9, 25, 41, 53, 56, 59, 62, 73, 76, 79, and 82, Ramamurthy teaches

- wherein the generic application-layer network protocol is hypertext transfer protocol (column 8, columns 48-49).

Regarding claims 10, 26, 42, 54, 57, 60, 63, 74, 77, 80, and 83, Ramamurthy teaches

- receiving at the server a signal representing data in response to the second request; and
- sending from the server a signal representing at least a portion of the data to the remote user (columns 8-9, columns 48-49).

Regarding claims 11, 27, 43, 55, 58, 61, 64, 75, 78, 81, and 84, Ramamurthy teaches

- wherein the first secure resource includes a Web site, and the data is hypertext mark-up language (column 8, columns 48-49).

Regarding claims 4, 20, 36, 51, and 71, Ramamurthy teaches

- wherein the request includes a logon credential for the remote user, the method / apparatus further comprising:
- authenticating the remote user based on the logon credential before sending the second request (column 7, column 8, lines 3-41, columns 48-49).

Regarding claims 5 and 21, Ramamurthy teaches

- wherein the request includes a logon credential for the remote user and the type of security credential required to access the first secure resource includes the logon credential,
- the method / apparatus further comprising:
- sending the signal representing the second request to retrieve the first secure resource, the second request including the logon credential (column 7, column 8, lines 3-41, columns 48-49).

Regarding claims 28 and 65, Ramamurthy teaches

- wherein the means for receiving includes means for receiving at the server a signal representing a third request from the remote user for a

Art Unit: 2136

second secure resource residing on the network (columns 8-9), the apparatus further comprising:

- means for determining, without the intervention of the user, the type of security credential for the remote user that is required to access the second secure resource (column 8, lines 3-41, column 48, lines 38-67, column 49, lines 1-45); and
- means for sending from the server a signal representing a fourth request to retrieve the second secure resource (column 8, lines 3-41, column 48, lines 38-67, column 49, lines 1-45),
- the fourth request including a second of the security credentials for the user of the type required to access the second secure resource; and
- wherein the signals representing the second and fourth requests are sent concurrently (column 8, lines 3-41, column 48, lines 38-67, column 49, lines 1-45).

Regarding claims 13, 29, 45, and 66, Ramamurthy teaches

- wherein the types of security credentials included in the second and fourth requests differ (columns 8-9).

Regarding claims 14, 30, 46, and 67, Ramamurthy teaches

- wherein the types of security credentials included in the second and fourth requests are the same (columns 8-9).

Regarding claims 31 and 68, Ramamurthy teaches

- receiving at the server a signal representing the first security credential from the user before receiving the signal representing the first request (columns 8-9).

Regarding claims 37, 52, and 72, Ramamurthy teaches

- wherein the request includes a logon credential for the remote user and the type of security credential required to access the first secure resource includes the logon credential,
- wherein the method further comprises:
- sending from the server the signal representing the second request to retrieve the first secure resource, the second request including the logon credential (columns 8-9).

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2136

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

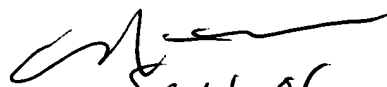
16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

17. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

18. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DGC

**NASSER MOAZZAMI
PRIMARY EXAMINER**


8/4/06